EXHIBIT 1

EnCase keeps tabs on compliance complexity | InfoWorld | Review | 2004-10-08 | By Oliver Rist,Brian Chee

About InfoWorld : Advertise : Subscribe : Contact Us : Awari

InfoWorld

PRODUCT REVIEWS GUIDE | REVIEWS | ANALYSES | SPECIAL REPORTS

HOME | NEWS | TEST CENTER | OPINIONS | PRODUCT GUIDE | TECHINDEX

The HP Compaq dc7600 with dual-core processing power.

» LEARN MORE

intel Pentium D inside

hp invent

⊙ Site ○ IT Product Guide

☐ Technology & Business |
☐ SOA Report

Enter Email Address

II

EnCase keeps tabs on compliance complexity

Flexible forensics tools closely tracks and records incidents

By Oliver Rist , Brian Chee
October 08, 2004

It's a sad fact that many a network manager will skip this review. This in spite of Sarbanes-Oxley, HIPAA, and Gramm-Leach-Bliley. This in spite of identity theft, corporate espionage, and a bucket full of other white-collar crimes. Network managers will avoid this review because these are worst-case scenarios, and it's easier not to think about them than it is to rationally consider their potential costs. Mitigating these costs, both soft and hard dollar, is precisely what **Guidance Software's** (Profile, Products, Articles) EnCase Enterprise Edition is designed to handle.

Guidance Software describes EnCase as a "network-enabled forensics, incident response, and security analysis tool." Not only capable of ensuring your systems are properly patched, EnCase is fed by your intrusion detection system to closely track attacks and record them with snapshots for later review. Further, EnCase is an excellent tool for automating compliance testing for stringent regulations such as HIPAA. Companies can quickly search through servers and workstations from a single console for sensitive documents and images, then determine how files have been distributed through the enterprise and by whom.

SEE ALSO
• **Government publishes HI standards**
• **Cutting the Sarbanes-Oxl**

FIND PRODUCTS AND COM

TECHNOLOGY INDEX
• Applications
• Application Development
• Security
• Networking
• Wireless
• Platforms
• Hardware
• Data Management
• Storage
• Web Services
• Business
• Telecom
• Professional Services
• Standards

TECH WATCH

EnCase keeps tabs on compliance complexity | InfoWorld | Review | 2004-10-08 | By Oliver Rist,Brian Chee

Guidance Software, http://guidancesoftware.com/

Very Good 7.7

criteria	score	weight
Features	9	25%
Manageability	7	20%
Performance	8	20%
Integration	7	15%
Documentation	7	10%
Value	7	10%

Cost:
$1,600 per seat, as tested

Platforms:
Linux (Kernel 2.4), Solaris v8 and v9 (32-bit and 64-bit), Windows NT/2000/XP/2003

Bottom Line:
EnCase's roots in law enforcement combined with its capability of integrating with enterprise intrusion detection systems makes this one of the more flexible and easily integrated forensic solutions for the enterprise. Although it's very complex, this type of software is a must-have for companies faced with compliance issues.

About our Reviews and Scoring Methodology

EnCase consists of three components: the SAFE (Secure Authentication For EnCase) Server, the Examiners, and the Servlets. Using a police metaphor, the SAFE Server can be viewed as headquarters. This server manages authentication and secure communication among all other system components and stores EnCase log files for future analysis. The Examiners can be looked at as precinct houses. They're in charge of specific network segments or resources, depending on how you've architected your EnCase deployment. They also act as command consoles for analysis and incident response. The Servlets are the field detectives. They're installed on all EnCase-protected servers and workstations running OSes including Linux, Solaris, and Windows. Servlets watch out for trouble, gather information, and send out alerts.

Each component communicates using TCP/IP port 4445 with asymmetrical encryption (certificates) and simultaneous examiners and SAFE Servers you want for your enterprise. Licensing depends upon how many simultaneous examiners and SAFE Servers you want for your enterprise. With a single license, only one person at a time may examine data. This is certainly a flexible design, but it means that there's no such thing as a typical EnCase installation; pricing can vary widely from organization to organization.

Casing the Joint

We tested EnCase in the wild, opening it up to four different class C subnets across the University of Hawaii's production network. Once installed, we used EnCase to run vulnerability and patch compliance tests against our Linux and Windows test machines.

The Examiner station also allowed us to browse files on each machine. This feature includes the capability of displaying thumbnails of any images stored on the machine, whether current or recently deleted. We also compared the hash values from EnCase's library to determine whether any sensitive files, such as the Windows directory or the virus scanner, had been modified. This often occurs in Trojan horse attacks, in which malware substitutes critical files with corrupted ones.

EnCase also allowed us to search for known corrupted or attack-based files on our machines using keywords, hash values, hex strings from headers and partial headers; we also could search with manual browsing.
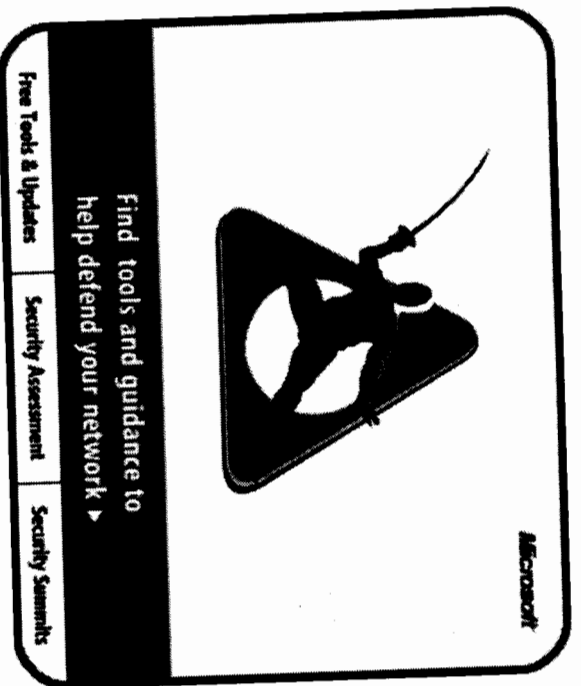
Searching for specific documents requires subject-matter expertise on the part of the user in order to formulate the properly phrased search questions; the well-designed GUI makes this easier. Admins can delegate search authority to different people within the organization; the HR administrator, for instance, might appropriately be given rights to search through all HR documents.

Find tools and guidance to help defend your network ▶

Free Tools & Updates | Security Assessment | Security Summits

Microsoft

Jon's Blog | Jon's Column

JON UDELL'S CORNER
Sidestepping th
(InfoWorld) - On a
"The West Wing,"
security adviser K
McCormack) repr

Telecommuters are less sec
People who work remotely are
productive, they are more likel
Don't take my word for it - tha
survey by Insight Express and
reported in EE Times. While 7
employees surveyed ...

Compuware plans EclipseCo
The EclipseCon 2006 conferen
the week of March 20 in Santa
and it looks like Compuware hi
this event. Compuware and Ec
representatives are being mos
about Compuware's plans. But

» MORE COLUMNISTS

MORE INFOWORLD BLOGS

COLUMNISTS
Dell gets petitioned, HP's f
(InfoWorld) - Gre
Microsoft is rollin
of vista when it a
millennium....

Open Sources
Is selling your open source ticket to freedom?
(InfoWorld)
Sarah Lacy's Open Season On
talks about some of the recent
acquisitions and the impact th

The Deep End
DNSBL Stats
For an upcoming article, I foun
to gather some statistics on DI
spamhaus.org, sorbs.net, and

EnCase keeps tabs on compliance complexity | InfoWorld | Review | 2004-10-08 | By Oliver Rist,Brian Chee

EnCase also features EnScript, a Perl/Java-like scripting language. Using EnScript, admins can customize searches of any combination of single or multiple machines for all documents meeting specific criteria, including size, keywords, extension type, and even the destination of the data. Thus an admin could craft a script that tracks documents containing the keywords "social security number" and whether an employee attempts to distribute them to improper departments or outside the organization.

Administrators can set up EnCase to automatically monitor specific machines or groups for certain conditions, such as file alterations, rapid port probes, and more. If EnCase detects these activities, it can grab snapshots of the machine while the attack is in progress. By simply looking at a case file, admins can clearly view at a later time the attack's entire progression. EnCase can be integrated with **Internet Security Systems'** (Profile, Products, Articles) intrusion detection product or Snort for managing attack thresholds, making the feature all the more useful.

Case evidence and disk snapshots can be stored on just about any file system you wish. Snapshot information can also be mounted as a read-only volume, designed as a way to gather immediate evidence for later analysis.

Using the stand-alone EnCase Professional Edition, you can produce a case file to submit to a local law enforcement agency. Case files can pertain to any number of incidents, such as a worm break or a case of an employee sending sensitive documents to an inappropriate recipient. Case files can contain various types of data, and they're locked up and protected from unauthorized access. In a nice touch, these case files are open enough to accept additional data from other EnCase instances.

Additionally, each Examiner account can be given varying levels of access to examination functions. So a junior engineer might only able to take and store system snapshots, whereas a user with higher access privileges can later peel apart the images to create the case evidence.

Although the field of corporate computer-forensic products is rather new, the EnCase software is surprisingly mature. Installation completed without incident, and even during operation we encountered only minor hiccups. For instance, it didn't correctly identify our Linux test machine as running Slackware, but it did correctly identify the Linux kernel version.

Also, EnCase didn't directly support FreeBSD, one of the other platforms on which we tested. However, we were able to work around that, because EnCase allows admins to perform a manual forensic copy, which is essentially taking a snapshot of the entire disk image (regardless of OS) using a directly attached slave drive, or a USB or network connection.

Finally, EnCase is remarkably complex. The company might seriously consider producing some tutorials on CD or some documentation featuring example data.

Forensic software such as EnCase began in the law enforcement field. But with the grave increase in computer crime -- especially from inside the firewall -- such systems are often necessary for effective security. Further, EnCase provides an easy and centrally managed method for compliance testing with an automatic results store thrown in. For many enterprises, solutions such as EnCase might be considered a security luxury; but for trading companies, banks, and even companies that merely keep a large amount of customer financial data, EnCase is a must.

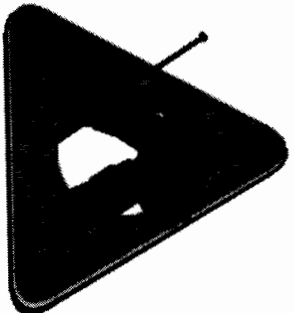*Oliver Rist is a senior contributing editor at InfoWorld.*

- **Advice Line**
- **Database Underground**
- **The Deep End**
- **Enterprise Mac**
- **Grid Meter**
- **The Gripe Line**
- **InfoWorld Daily**
- **Inside IT**
- **IT Troubleshooter**
- **Jon's Radio**
- **Open Sources**
- **Real World SOA**
- **Security Adviser**
- **SMB IT**
- **The Storage Network**
- **Tech Watch**
- **Zero Day**

IDG ENTERPRISE NETWORK
- Riding The California Priva

GOVERNMENT IT & POLICY
- In One Ear, Out the Othe Drivers
- Sourcefire Officials Hopef
- Universal Stem Cell Princi

EnCase keeps tabs on compliance complexity | InfoWorld | Review | 2004-10-08 | By Oliver Rist,Brian Chee

TOP NEWS:

VIRUSES

Free Tools & Updates | Security Assessment | Antivirus Protection

» Cell phone ticketing coming to Germany
The airline DBA's passengers will be able to check in and board flights on the Munich-Hanover route with mobile phones capable of receiving MMS

» Borland: Interest, but no buyer yet, for tools line
Executive details intentions, provides progress report on sale of developer tools

» Intel gives earnings warning
Intel faces increasing competition from AMD

» Update: Google shrinks further the Mini search device
Google introduces its lowest-priced search device to date

» HP Labs India working to bridge TV and Internet
Also in Brief: OSS/J names Vodafone D2 exec as new chair; IBM readies SOA packages; Intel to invest $300M in Vietnam chip plant; SOA, Forum integrate products; Ericsson sues Samsung in patent dispute; Sony, NEC to establish optical disc joint venture; Orange offers wireline service

» Vendors form new OpenDocument alliance
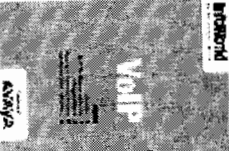ODF could have provided support to embattled CIO who planned Massachusetts' migration to OpenDocument

VoIP
Learn how to successfully plan, deploy and manage an effective VoIP system. This new InfoWorld IT Strategy Guide is available at no charge for a limited time, compliments of Avaya. Download now.
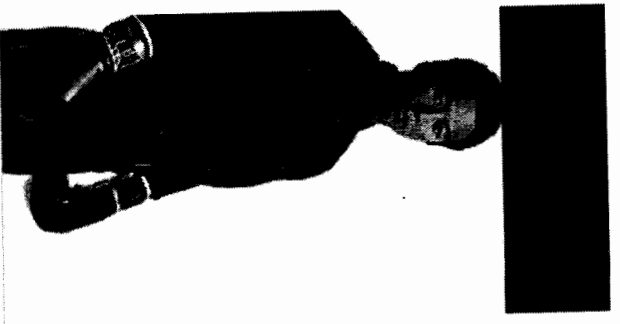
» Click here to download now

EnCase keeps tabs on compliance complexity | InfoWorld | Review | 2004-10-08 | By Oliver Rist,Brian Chee

- Special Advertising Partners -

WHITE PAPERS

» **The Business Value of HP-UX 11i: HP-UX 11i vs. Linux** - Today there are many choices of operating system platforms and servers to help meet the challenges of lowering costs and meeting higher adaptability requirements. Many organizations are considering ...

» **HP-UX 11i: A Foundation for Enterprise Computing That Delivers Business Agility Through Integrated Virtualization, Workload Management, and Enhanced Security** - Today's enterprise customers want their IT environments to support higher levels of business agility and deliver more business value. This white paper will discuss how the latest release of HP's ...

» **Migrating to Converged Networks and IP Telephony Applications** - This paper explores the new requirements that migration to converged voice and data networks is creating for IP Telephony architectures and their operation and management.

» **Exploring Alternative Convergence-Ready Solution**

» **Solving the Enterprise Mobility Challenge**

» **New Era of Intelligent Communications: Executive Presentation**

MORE SECURITY WHITE PAPERS

» **Start a VisOps Based Change Management Program**
Shortcuts for jumpstarting your change management program.

» **The PCI Data Standard: It's Everywhere You...**
Tripwire solutions can help organizations achieve PCI regulatory compliance - specifically in the ...

» **Database Encryption: Securing Critical Data**
Encrypting critical data in databases can help organizations address goals for compliance & ...

» **Security best practice in regulated industries**
Security experts Susan Orr and Paul Reymann (co-author of GLBA) explore how SIEM increases an ...

» **Improve your overall IT security through SIEM**
Learn how eIQnetoworks help organizations meet increasing security operations challenges through the ...

SPONSORED LINKS

» **Verizon Business** - Total capability backed by accountability

» **HP** - HP Workstations for Financial Markets

» **Microsoft** - Microsoft Free Security Tools & Updates

» **SSA Global** - Start responding to customer demand in real time. Now.

» **Informatica** - The Data Integration Company

INFOWORLD MARKETPLACE

>> WHITE PAPERS LIBRARY

WHITE PAPERS E-MAIL ALERT
Find out when the latest white paper is available:

E-mail Address

WHITE PAPERS BY TOPIC

• Application development
• Applications
• Business
• Hardware
• Networking
• Platforms
• Security
• Standards
• Storage
• Telecom
• Web services
• Wireless

EnCase keeps tabs on compliance complexity | InfoWorld | Review | 2004-10-08 | By Oliver Rist,Brian Chee

Page 6 of 7

» **Disaster Recovery Seminar**
Network with other Symantec Users. Discuss Ideas and Share Solutions!

» **System Management for new Enterprise environments**
Request white paper which outlines the case for an IT Portal architecture to meet the new ...

» **Secure & Easy Console Management with Digi CM**
The Digi CM console server provides secure, intelligent & easy access to network devices with a ...

» **Security Within - Configuration based Security**
Configuration and policy based security systems are a pro-active way to defend against IT security ...

» **Need to track and control Web usage at work?**
All organizations need to monitor, analyze, track, and control workers' Web use. Our products do it ...

>> BUY A LINK NOW

FREE SUBSCRIPTION

Order today to get your **FREE subscription** (a
$195 value!) to InfoWorld magazine, the weekly
publication that provides indispensable product
information to IT professionals.

NOTE: Complimentary subscriptions sent only to
those applicants who qualify.

First Name: _____   Last Name: _____

Company Name: _____   Title: _____

Mailing Address: _____

State/Province: City: _____
Select One

Email Address: _____   Zip/Postal Code: _____

NOTE: Offer valid in U.S. and Canada only
Non-U.S. click here

| **HOME** | **NEWS** | **TEST CENTER** | **OPINIONS** | **PRODUCT GUIDE** | **TECHINDEX** |

About :: Advertise :: Subscribe :: Contact Us :: Awards :: Events

http://www.infoworld.com/article/04/10/08/41TCencase_1.html?s=feature

3/3/2006

EnCase keeps tabs on compliance complexity | InfoWorld | Review | 2004-10-08 | By Oliver Rist,Brian Chee

site: testcenter zone: feature pkeys: pkey=security; skeys: skey=computer_forensics;skey=patch_management; tdata: kw=; tid:

Page 7 of 7